Risk Assessment and Management, Tools and Applications

Dr. Michael G. Stamatelatos
Manager, Risk Assessment
NASA Headquarters
Office of Safety and Mission Assurance
mstamate@hq.nasa.gov
(202) 358-1668

Outline

- Risk and Risk Assessment
- Continuous Risk Management Process
- NASA Risk Management Requirements
- Probabilistic Risk Assessment (PRA) Methods
- PRA Application Example

Decision Under Uncertainty

- ⇒ **Most decisions, especially complex ones, are made under some degree of uncertainty**

- ⇒ **Risk assessment and management have therefore been performed either implicitly or explicitly in all rational decisions regarding complex systems and activities that have involved many stakeholders**

- ⇒ **Following is an interesting example from history**

Risk Assessment & Management in History

"We the Athenians in our persons, take our decisions on policy and submit them to proper discussion. The worst thing is to rush into action before the consequences have been properly debated. And this is another point where we differ from other people. We are capable at the same time of taking risks and estimating them beforehand. Others are brave out of ignorance, and when they stop to think, they begin to fear. But the man who can most truly be accounted brave is he who best knows the meaning of what is sweet in life, and what is terrible, and he then goes out undeterred to meet what is to come."

from Pericle's Funeral Oration in Thucydides'
"History of the Peloponesian War"

This is an excerpt from a speech of Pericle, Athenian general, to his troops before a battle in the war between Athens and Sparta that started in 431 B.C..

Motivation: Why Perform PRA?

In many modern technological applications (e.g., electric power generation, chemical processing industry, etc.), Probabilistic Risk Assessment (PRA) has proven to be a systematic, logical, and comprehensive tool to assess risk (likelihood of unwanted consequences) for the purpose of:

⇒ **Increasing safety in design, operation and upgrade**

⇒ **Saving money in design, manufacturing or assembly and operation**

Necessity of PRA at NASA

At NASA, PRA is necessary (N) and/or appropriate (A) for:

	N	A
• Obtaining Presidential approval for launch of certain quantities of nuclear materials (e.g. Galileo, Ulysses, Cassini)	X	X
• Analytically demonstrating satisfaction of planetary protection requirements (e.g., Mars Sample Return)	X	X
• Supporting decision making for design and modification of systems in NASA missions (e.g., Space Shuttle, ISS, CRV)		X

In fact, NASA has performed, is performing, or intends to perform PRA for most of the preceding examples

What is Risk?

⇒ **GENERAL:**

Uncertainty associated with the realization of a non-certain outcome (goal, activity, project, etc.)

⇒ **SAFETY and SYSTEM:**

Frequency (probability per unit time) and severity of an undesired occurrence/consequence (end state). For safety applications, the consequence is illness or injury to individuals or groups of individuals.

Risk Versus Hazard in Safety Assessment

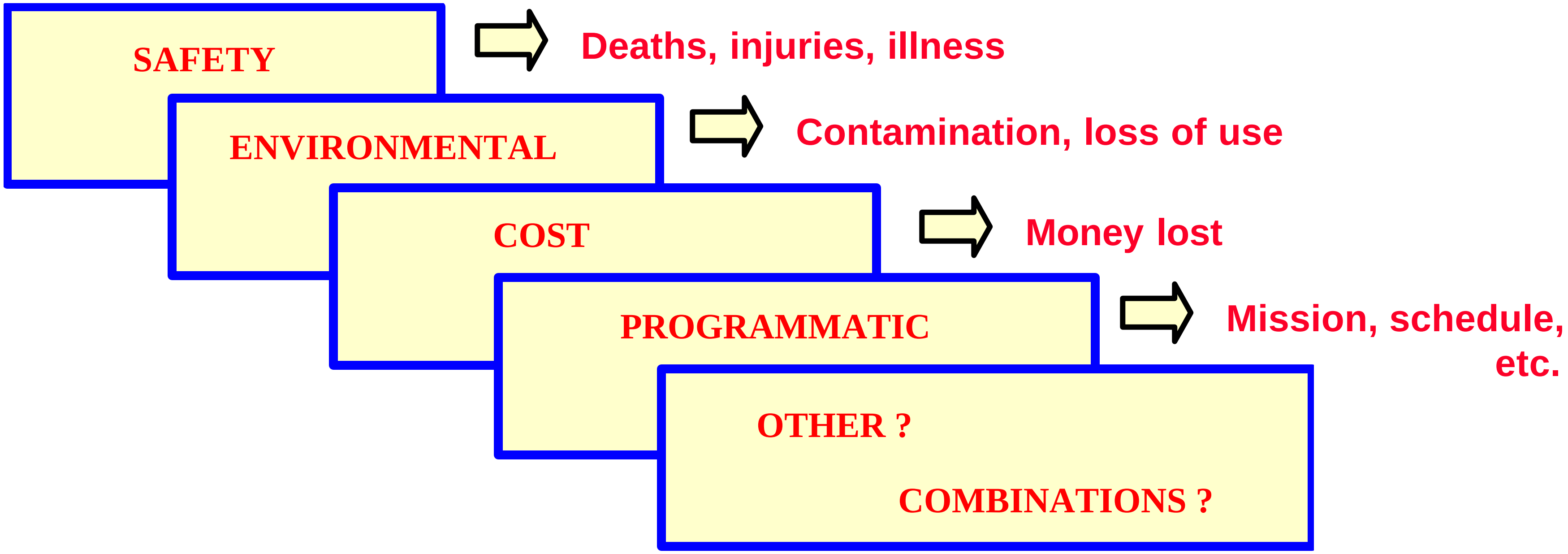
- ***Hazard*** **is a real/potential condition that causes: *injury* or *death* to people, *loss* of or *damage* to equipment, property, etc.**

  - **Hazard is a one-dimensional quantity characterized by *magnitude,* or *severity.***

- ***Risk*** **is the *likelihood* and the *magnitude,* or *severity*, of an undesired occurrence or consequence (end state)**

  - **Risk is a two-dimensional quantity.**

Types of Risk and Related Consequences



SAFETY → Deaths, injuries, illness

ENVIRONMENTAL → Contamination, loss of use

COST → Money lost

PROGRAMMATIC → Mission, schedule, etc.

OTHER ?

COMBINATIONS ?

Risk can be evaluated qualitatively or quantitatively

Qualitative Risk Representation

Frequency	Low	Medium	High
High	🟧	🟥	🟥
Medium	🟨	🟧	🟥
Low	🟩	🟨	🟧

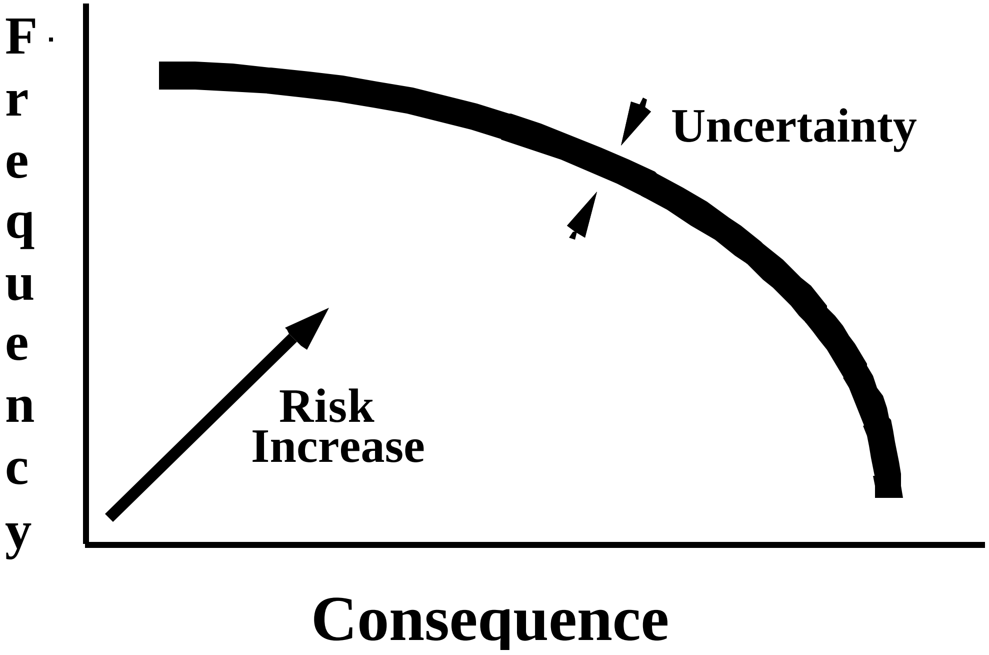
Consequence Severity

Mathematical Expression of Risk

$$\boxed{\begin{matrix}\text{RISK}\\[2em] \dfrac{\text{Detriment}}{\text{Unit Time}}\end{matrix}} = \boxed{\begin{matrix}\text{FREQUENCY}\\[2em] \dfrac{\text{Events}}{\text{Unit Time}}\end{matrix}} \times \boxed{\begin{matrix}\text{SEVERITY}\\[2em] \dfrac{\text{Detriment}}{\text{Event}}\end{matrix}}$$

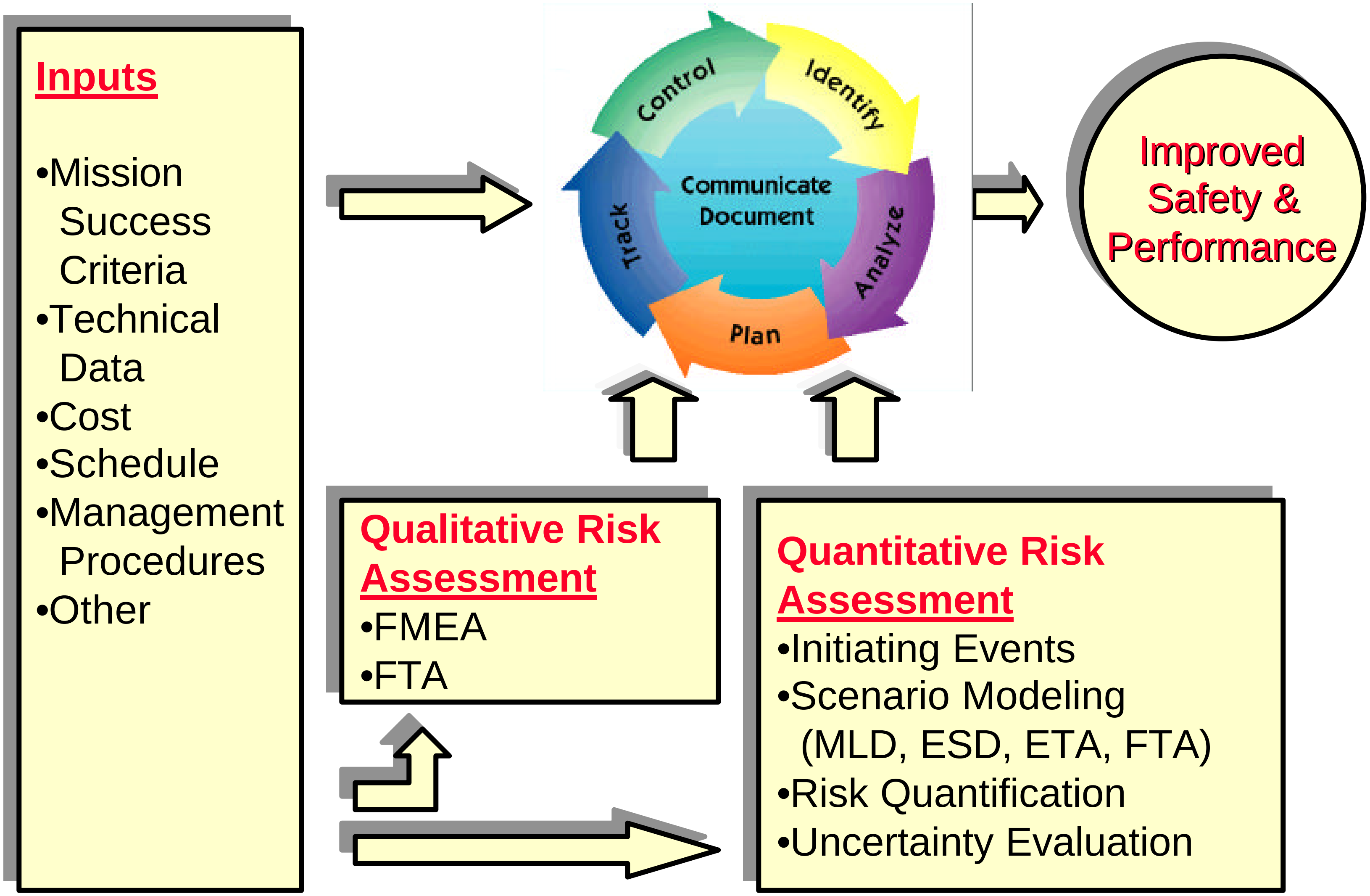
Note: Frequency is either number of events per unit time or, for rare events, the probability of occurrence per unit time

Graphic Representation - Risk Curve



In mathematical terms, the risk curve is the complementary cumulative distribution function (CCDF), i.e., the frequency of exceeding a given consequence severity

Risk Assessment and Management



Inputs

- Mission Success Criteria
- Technical Data
- Cost
- Schedule
- Management Procedures
- Other

Qualitative Risk Assessment

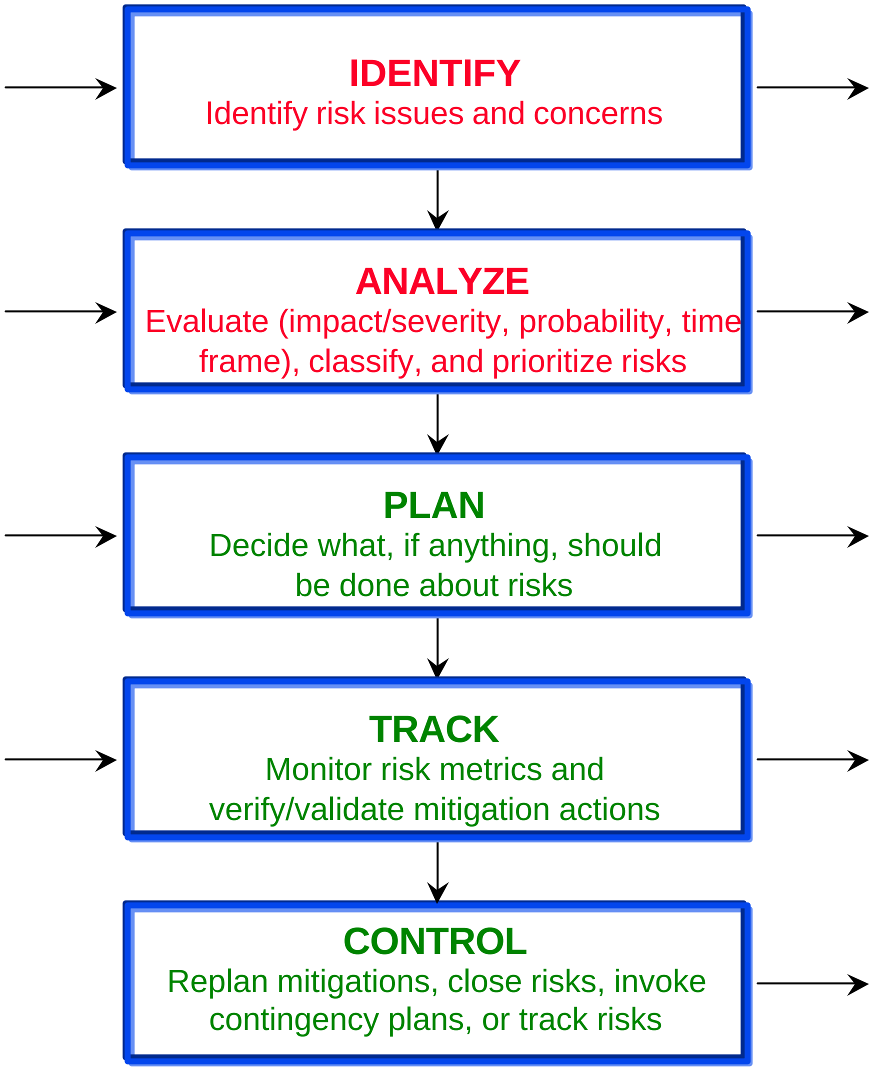
- FMEA
- FTA

Quantitative Risk Assessment

- Initiating Events
- Scenario Modeling (MLD, ESD, ETA, FTA)
- Risk Quantification
- Uncertainty Evaluation

Improved Safety & Performance

Risk Management Process



Program / Project constraints, hazard analysis, FMEA, FTA, lessons learned → **IDENTIFY** Identify risk issues and concerns → Statements of risk
List of risks

Risk data: test data, expert opinion, PRA, technical analysis → **ANALYZE** Evaluate (impact/severity, probability, time frame), classify, and prioritize risks → Risk evaluation
Risk classification
Risk prioritization

Resources → **PLAN** Decide what, if anything, should be done about risks → Risk mitigation plans
Risk acceptance rationale
Risk tracking requirements

Program/project data (metrics information) → **TRACK** Monitor risk metrics and verify/validate mitigation actions → Risk status reports on:
— Risks
— Risk mitigation plans

CONTROL Replan mitigations, close risks, invoke contingency plans, or track risks → Risk decisions

<u>Note</u>: Communication and documentation extend throughout all functions.

NASA Risk Management Requirements

- NPG 7120.5A, NASA Program and Project Management Processes and Requirements
  - **The program or project manager shall apply risk management principles as a decision-making tool which enables programmatic and technical success**
  - **Program and project decisions shall be made on the basis of an orderly risk management effort**
  - **Risk management includes identification, assessment, mitigation, and disposition of risk throughout the PAPAC (Provide Aerospace Products And Capabilities) process**
- NPG 8705.x (draft), Risk Management Procedures and Guidelines
  - **Provides additional information for applying risk management as required by NPG 7120.5A**

NASA Risk Assessment Requirements

- NPG 8715.3, NASA Safety Manual
  - Purpose of risk assessment is to identify and evaluate risks to support decision-making regarding actions to ensure safety and mission assurance
  - Risk assessment analyses should use the simplest methods that adequately characterize the probability and severity of undesired events
  - Qualitative methods that characterize hazards and failure modes and effects should be used first
  - Quantitative methods are to be used when qualitative methods do not provide an adequate understanding of failures, consequences, and events
  - System safety analysis must include early interaction with project engineering, integration, and operations functions to ensure all hazards are identified
  - The hazard assessment process is a principal factor in the understanding and management of technical risk
  - As part of the responsibility for overall risk management, the program/project manager must ensure that system safety analyses, appropriate to the program/project complexity, have been conducted

NASA Risk Assessment Requirements

- NSTS 22206, Instructions for Preparation of FMEA and CIL [for Space Shuttle]
  - System and performance requirements are defined
  - Analysis assumptions and groundrules are specified
  - Block diagrams (functional or reliability) are developed
  - Analysis worksheets which include identification of every failure mode are developed (the effects documented address the worst case.)
  - Corrective actions and design improvements are evaluated and recommended
  - Analysis is summarized in report form
- SSP 30234, Instructions for Preparation of FMEA and CIL [for Space Station]
  - FMEA process, requirements, rules, reporting requirements are described
  - CIL process, requirements, rules, reporting requirements are described
  - Ground support equipment FMEA and CIL processes, requirements, approvals, and databases are described

Risk Assessment Tools at NASA

- **NASA has been traditionally using two Risk Assessment (RA) tools for some time:**

  ___***Failure Modes and Effects Analysis (FMEA)***

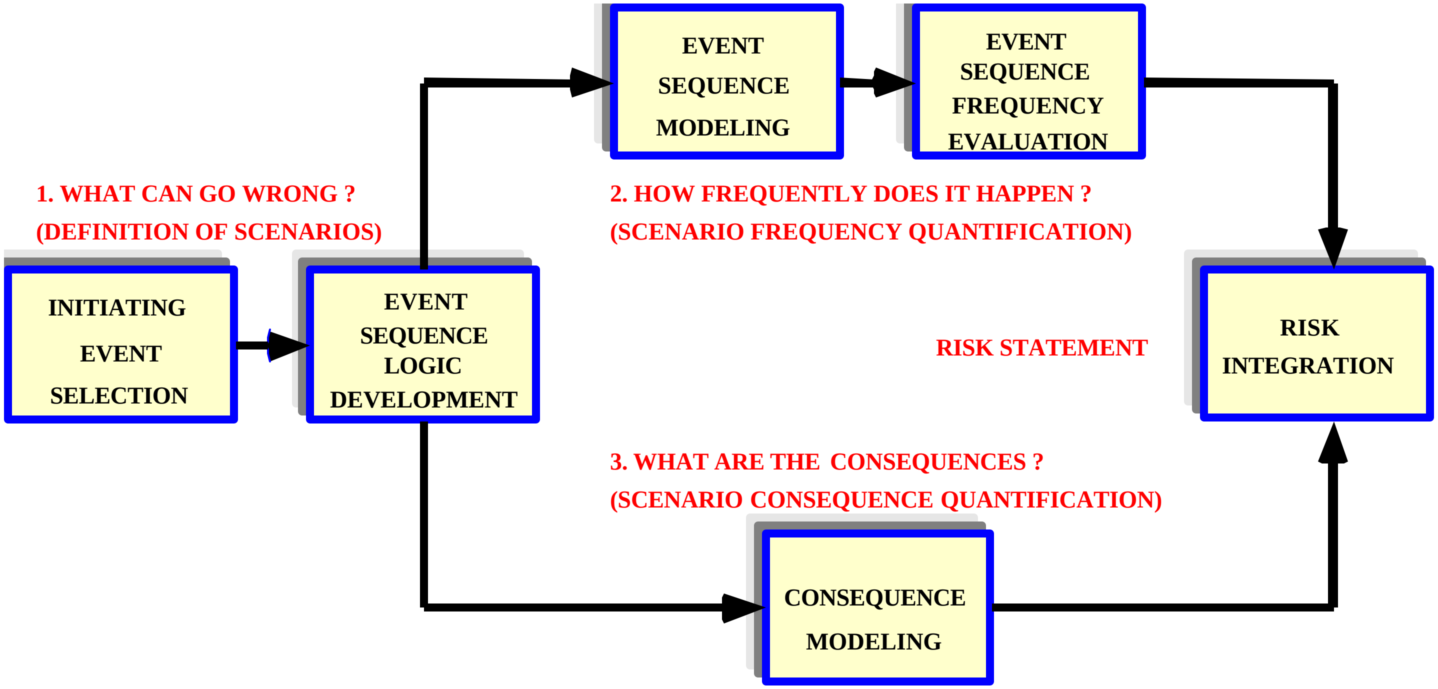
  Fault Tree Analysis (FTA)

- **NASA has been been broadening its repertoire of RA tools and has began to systematically use a more comprehensive set of tools collectively called**

  Probabilistic Risk Assessment (PRA)

  PRA is a systematic, logical, comprehensive discipline that uses tools like FMEA, FTA, Event Tree Analysis (ETA), Event Sequence Diagrams (ESD), Master Logic Diagrams (MLD), Reliability Block Diagrams (RBD), etc. to quantify risk.

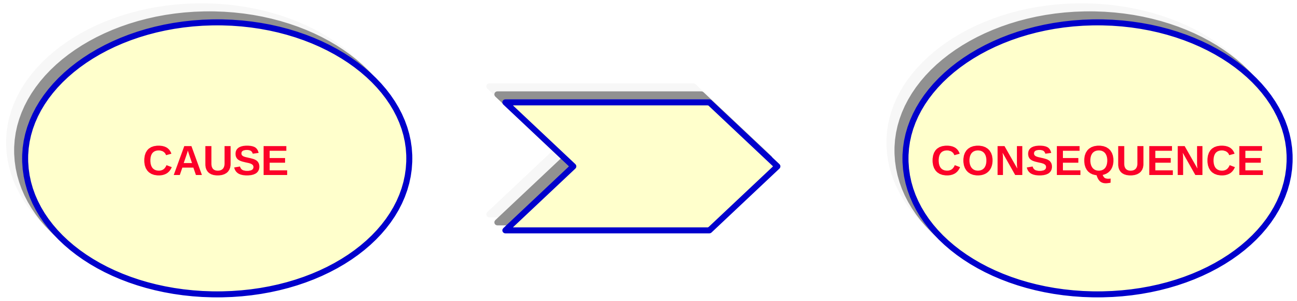
PRA Answers Three Questions


EVENT SEQUENCE MODELING
EVENT SEQUENCE FREQUENCY EVALUATION
1. WHAT CAN GO WRONG ?
(DEFINITION OF SCENARIOS)
2. HOW FREQUENTLY DOES IT HAPPEN ?
(SCENARIO FREQUENCY QUANTIFICATION)
INITIATING EVENT SELECTION
EVENT SEQUENCE LOGIC DEVELOPMENT
RISK STATEMENT
RISK INTEGRATION
3. WHAT ARE THE CONSEQUENCES ?
(SCENARIO CONSEQUENCE QUANTIFICATION)
CONSEQUENCE MODELING

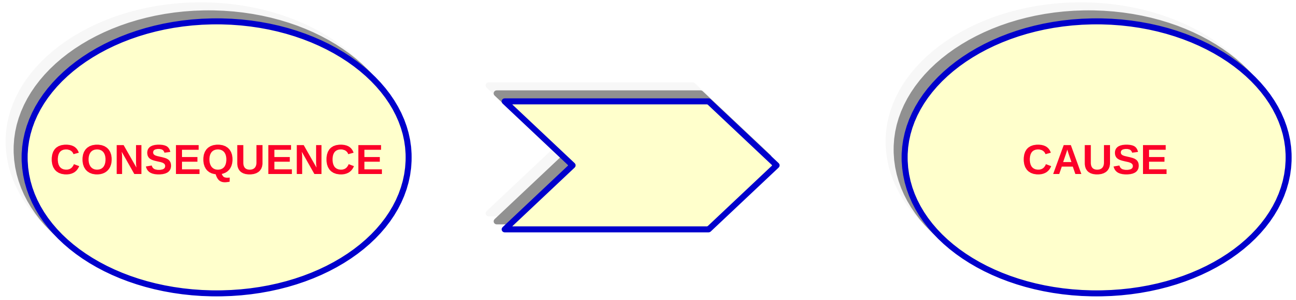
PRA is generally used for low-probability and high-consequence events for which insufficient statistical data exist. If enough statistical data exist to quantify system or sub-system failure probabilities, use of some of the PRA tools may not be necessary.

Inductive and Deductive Logic Tools

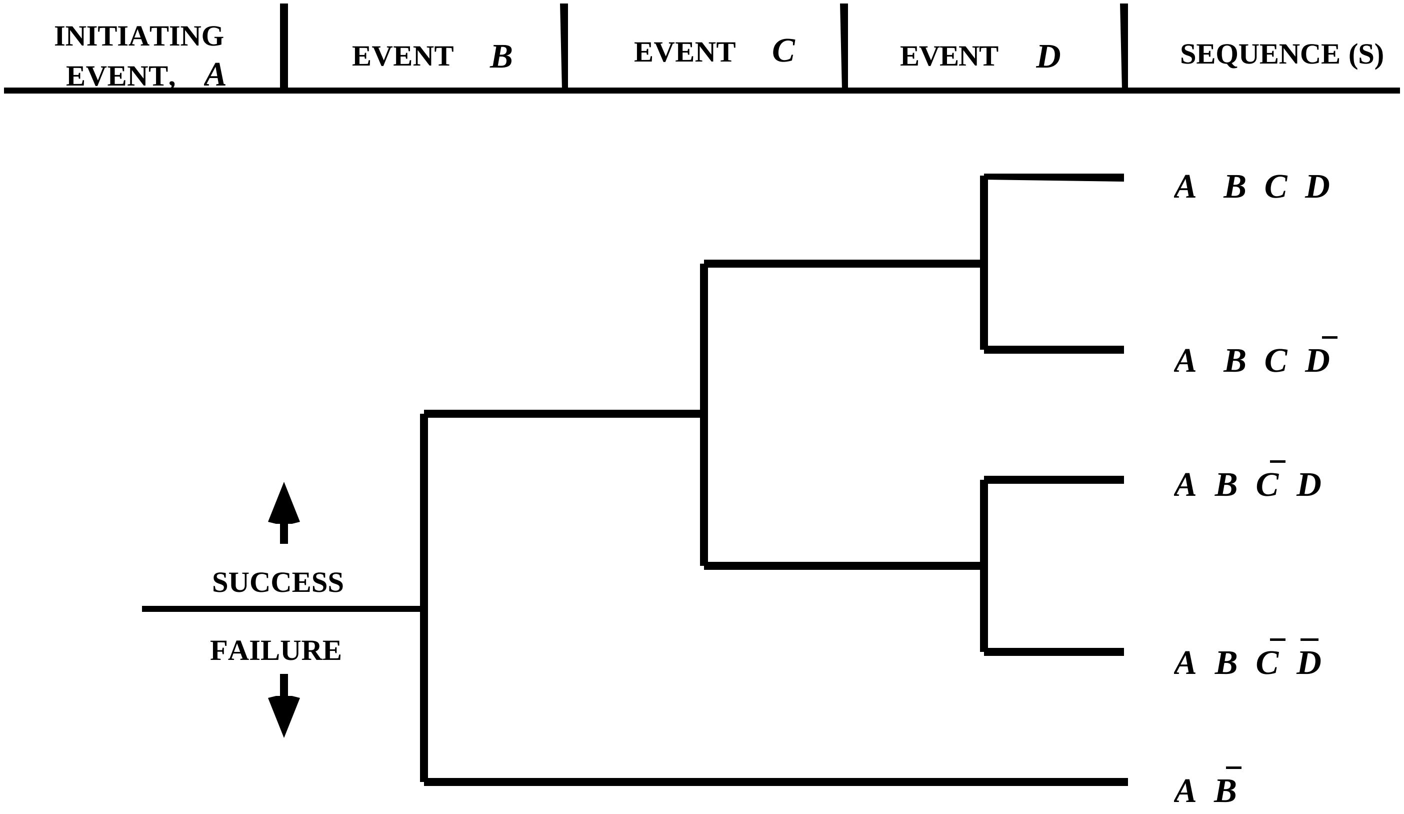
- **Inductive (Forward) Logic : FMEA, RBD, ESD, ETA**



- **Deductive (Reverse) Logic : MLD, FTA**



Event Tree



INITIATING EVENT, *A* | EVENT *B* | EVENT *C* | EVENT *D* | SEQUENCE (S)

SUCCESS

FAILURE

$A\ B\ C\ D$

$A\ B\ C\ \bar{D}$

$A\ B\ \bar{C}\ D$

$A\ B\ \bar{C}\ \bar{D}$

$A\ \bar{B}$

Cause (IE) → Consequences (S)

Inductive logic

Fault Tree

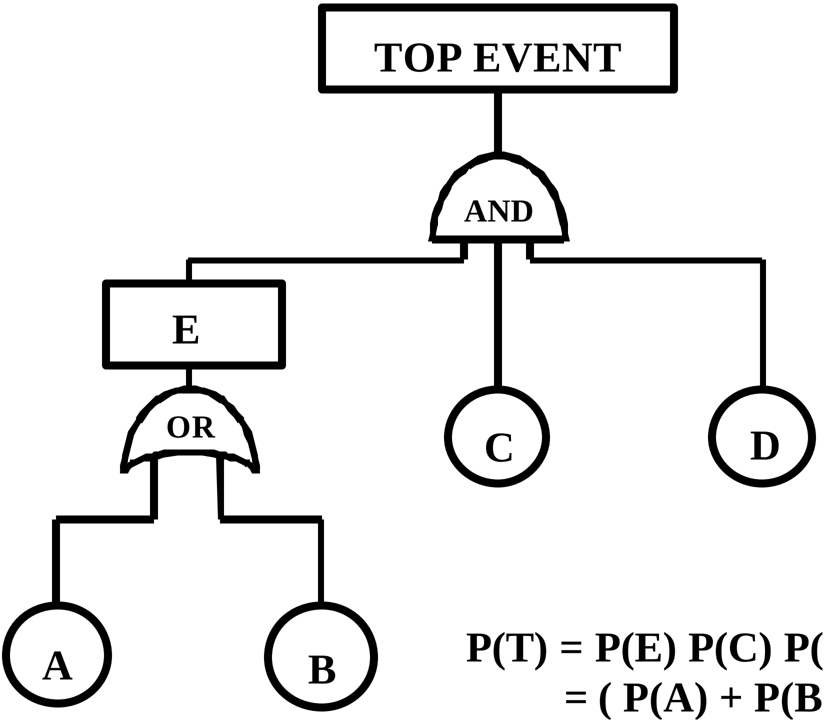
Top Event

Gate

Intermediate event

Gate

Basic events



Consequence (TE)

Deductive logic

Causes (A,B,C,D)

$$P(T) = P(E)\,P(C)\,P(D)$$
$$= (\,P(A) + P(B)\,)\,P(C)\,P(D)$$

Cut Sets: (A,C,D)   (B,C,D)

“Classical” PRA Methodology Flow

1. Identification of end-states of interest (related to PRA purpose)
2. System familiarization (“as-is” information) and data collection
3. Identification, selection, screening of initiation events, or IE, (may require high-order logic model; e.g., master logic diagram or MLD)
4. Definition and modeling of all scenarios linking each initiating event to the end states, using event sequence diagrams (ESD), or event trees (ET)
5. Modeling of pivotal events, the ET branch points; e.g., using fault trees (FT)
6. Risk quantification for each pivotal event and each scenario and risk aggregation for all like end states
7. Full uncertainty analysis and sensitivity analysis as needed
8. Risk importance ranking for risk reduction

Simple PRA Application

⇒ **Consider a plastics manufacturing plant that handles flammable and toxic materials in the production line.**

⇒ **The objective of this simple example is to show the application of the "classic" PRA process to the assessment of risk at the above-mentioned plant.**

⇒ **Specifically, we will examine the risk resulting from the occurrence of a fire at the plant and its impact on the continued plant operation (purpose of the PRA). The plant will be unsafe to operate if the fire cannot be prevented or contained and extinguished without causing harm to personnel, the plant and its surroundings.**

⇒ **Following is the application of the eight PRA steps outlined in the previous viewgraph.**

1. End States

The end states and the associated impacts of interest are:

1. **None or minor - Detrimental consequences of the undesirable occurrence (initiating event) are either insignificant or kept at a minimum so that there is no personnel injury and no debilitating property damage. The plant will be allowed to continue operation.**

2. **Major - Significant property damage as a result of the undesirable occurrence but there is no harm or injury to personnel. The plant needs to be temporarily shut down for repair.**

3. **Catastrophic - Several on-site personnel are harmed/injured (hospitalized) and the plant is severely damaged as a result of the undesirable occurrence. The plant must be shut down for an indefinite period of time.**

2. Plant Familiarization Includes

⇒ **Site and buildings layouts and diagrams**

⇒ **Operation flow diagrams**

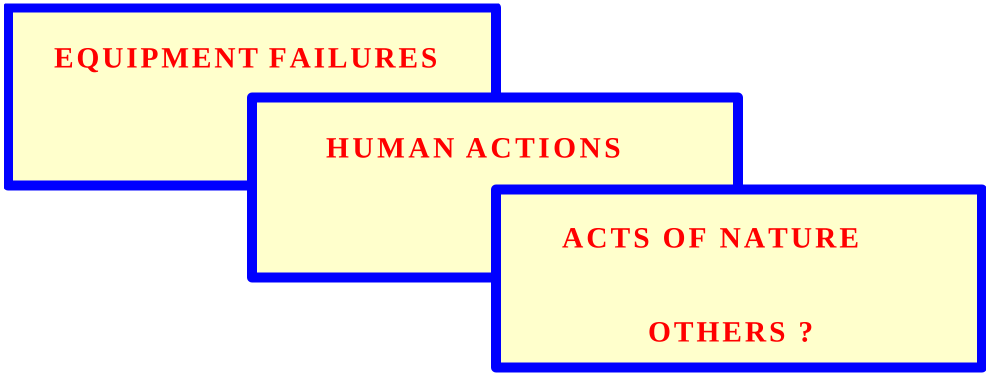
⇒ **Systems/equipment diagrams and engineering drawings**

⇒ **Physical inspection (walk-down) of the site and the plant buildings to determine the “as-is” rather than “as-built” status of the equipment**

⇒ **Normal operating and emergency procedures**

⇒ **Databases on: initiator frequencies, system and component reliability, maintenance, testing etc.**

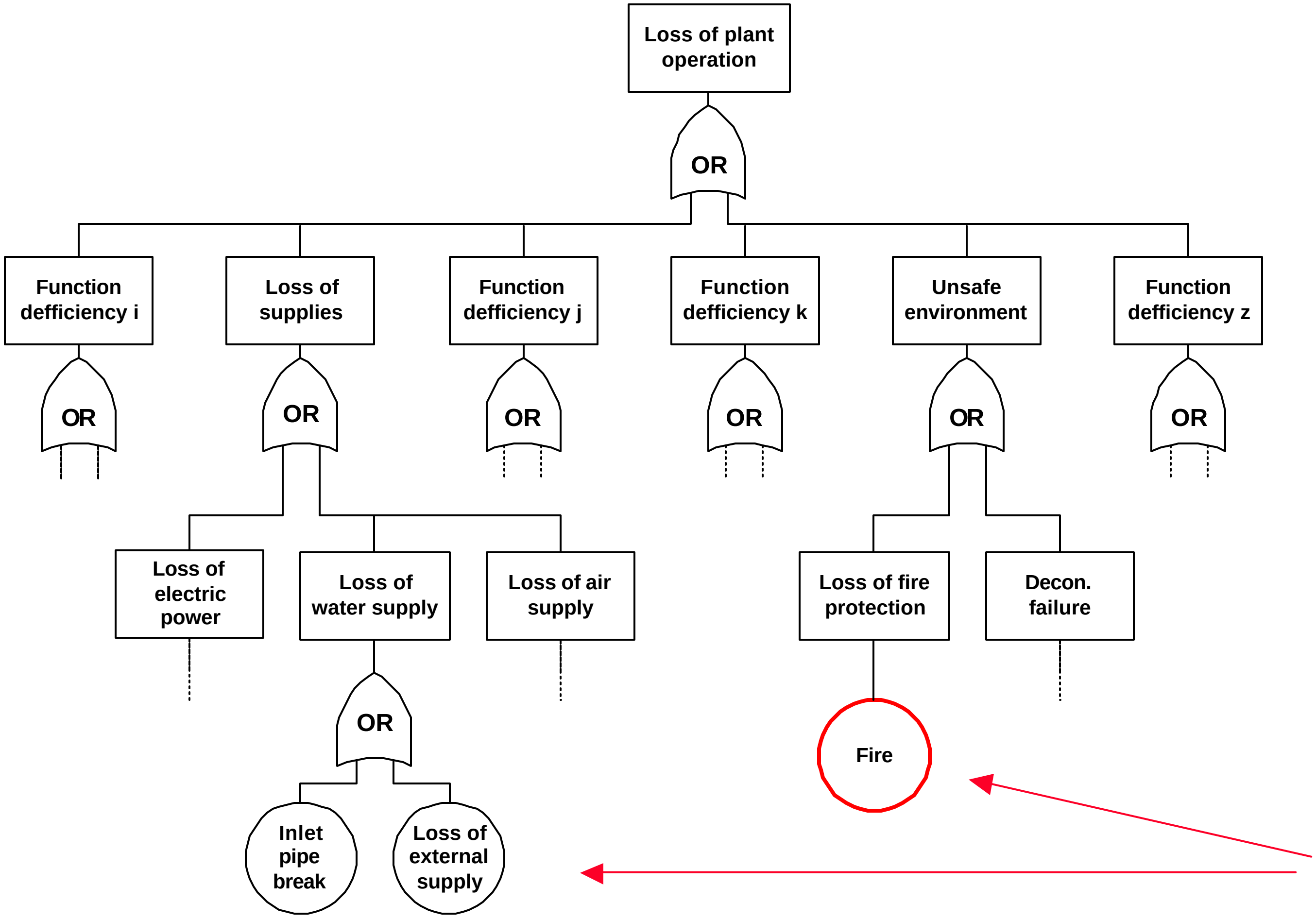
3. Initiating Events



Initiating events are the the first in a sequence of detrimental events leading to an adverse consequence.

In this particular case, the initiating event was a fire caused by the ignition of accidentally spilled flammable material (human action).

Master Logic Diagram (MLD)



Top event

Level 1

Loss of Function

Level 2

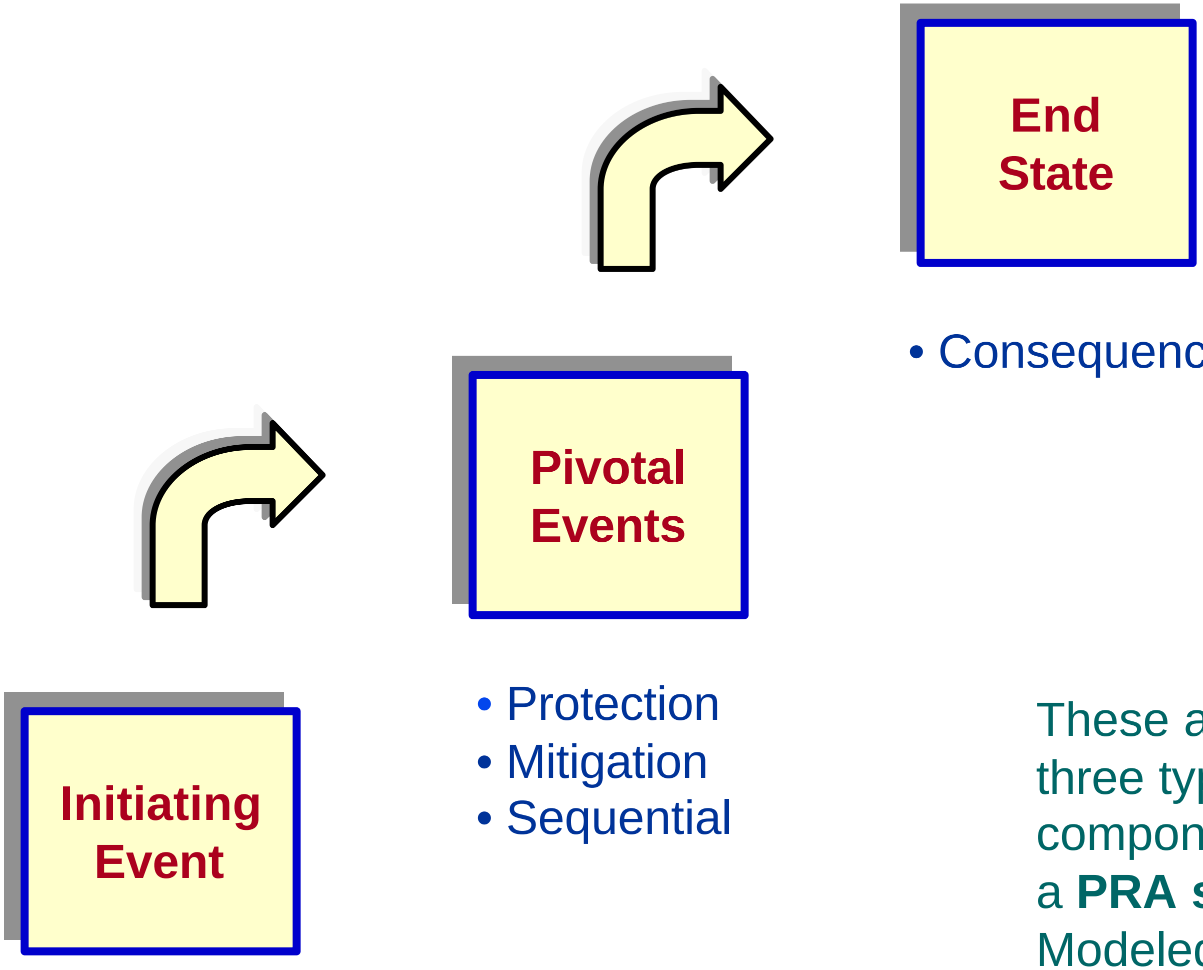
System Failure

……….

Level N

Initiators

4. PRA Scenario Structure



Initiating Event

- Cause

Pivotal Events

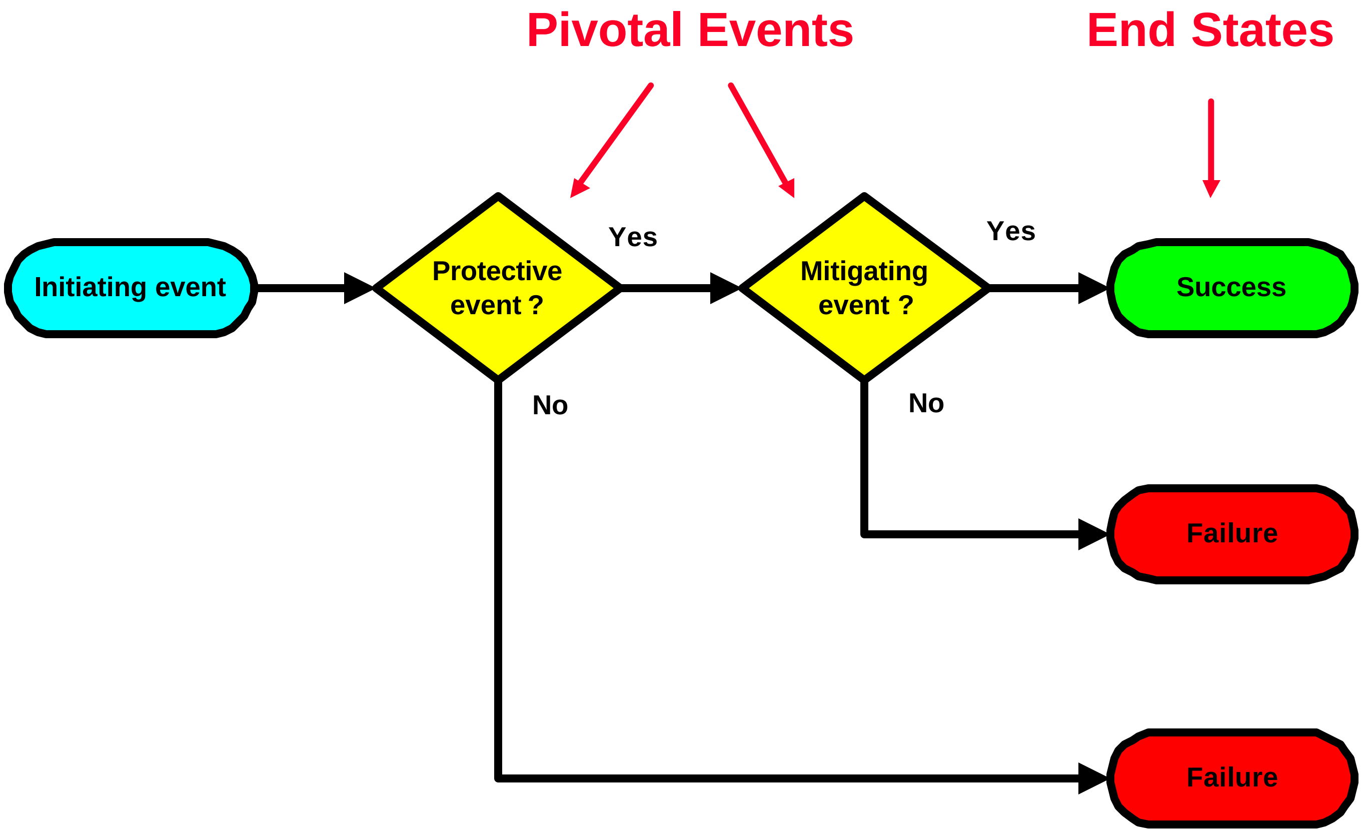
- Protection
- Mitigation
- Sequential

End State

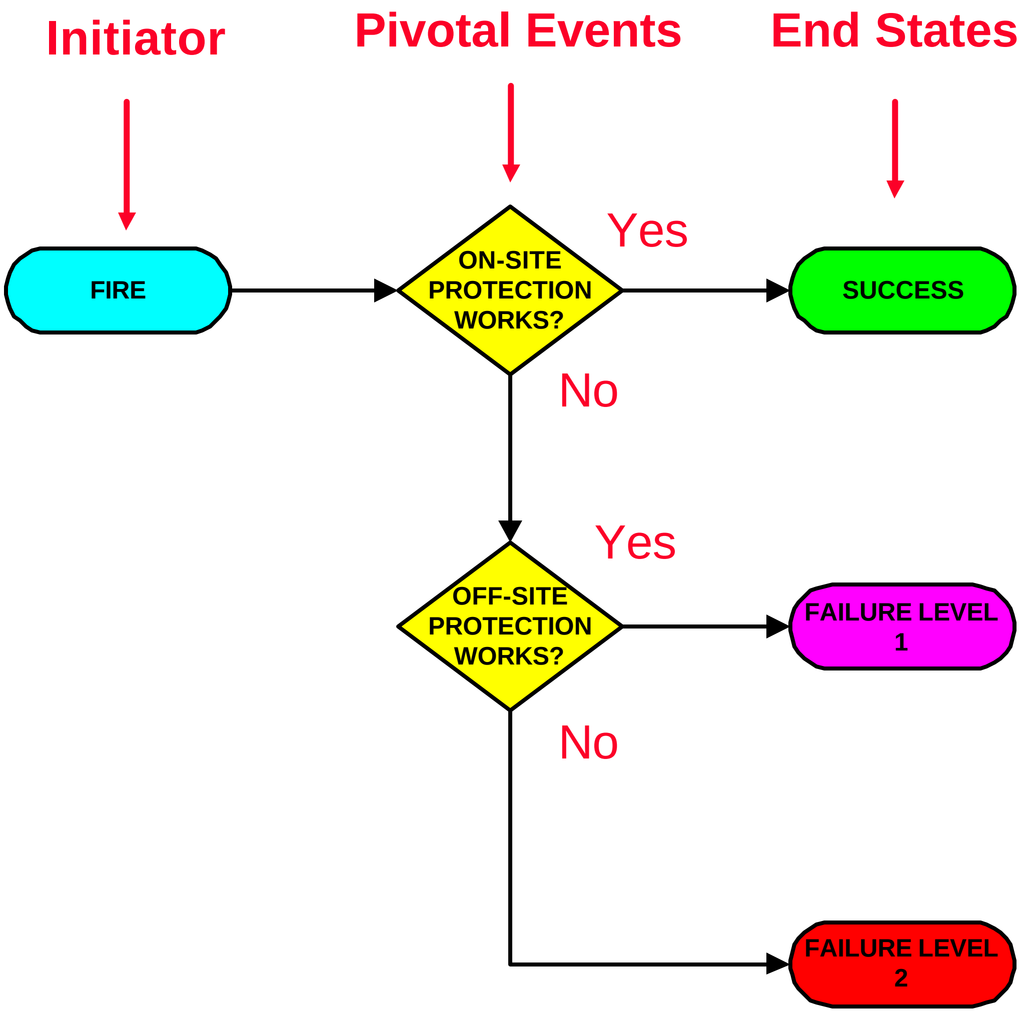
- Consequence

These are the three types of components in a **PRA scenario;** Modeled using ESD or ET

Event Scenario Development Process (ESD)



Event Sequence Diagram (ESD) Structure



Initiator

Pivotal Events

End States

FIRE

ON-SITE PROTECTION WORKS?

Yes

SUCCESS

No

OFF-SITE PROTECTION WORKS?

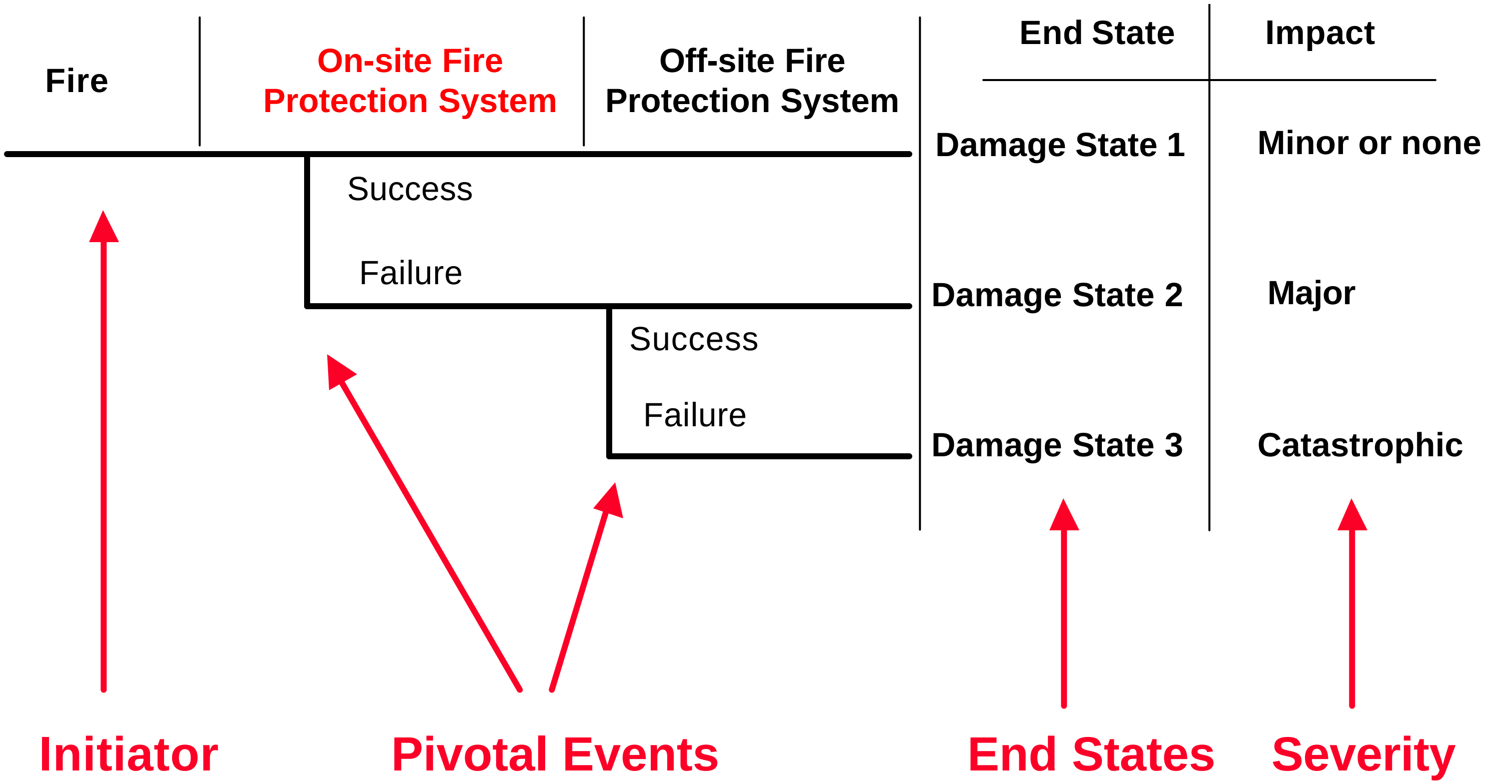
Yes

FAILURE LEVEL 1

No

FAILURE LEVEL 2

Scenario Modeling - Event Tree



Fire

On-site Fire Protection System

Off-site Fire Protection System

End State

Impact

Success

Failure

Success

Failure

Damage State 1

Minor or none

Damage State 2

Major

Damage State 3

Catastrophic

Initiator

Pivotal Events

End States

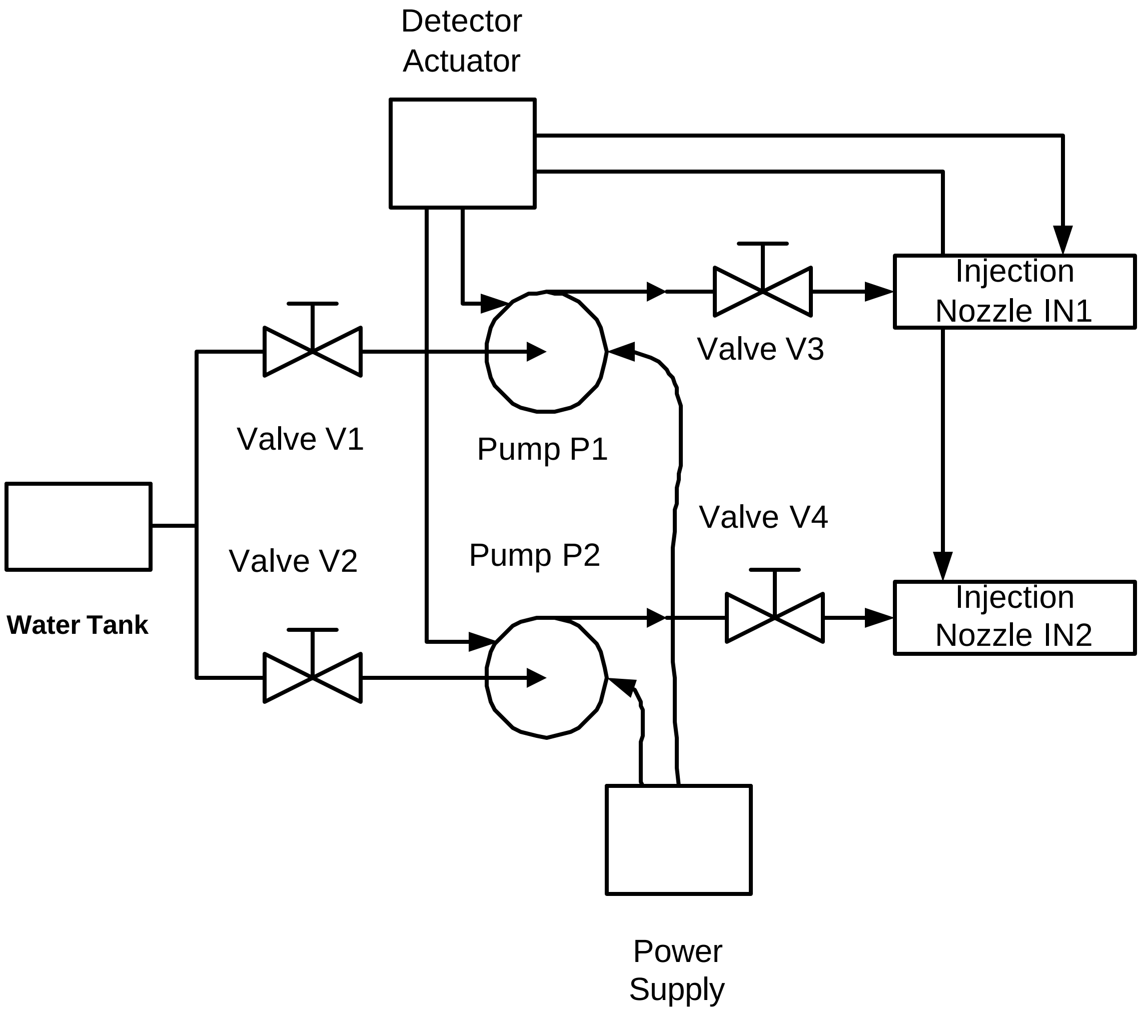
Severity

5. Pivotal Event Modeling

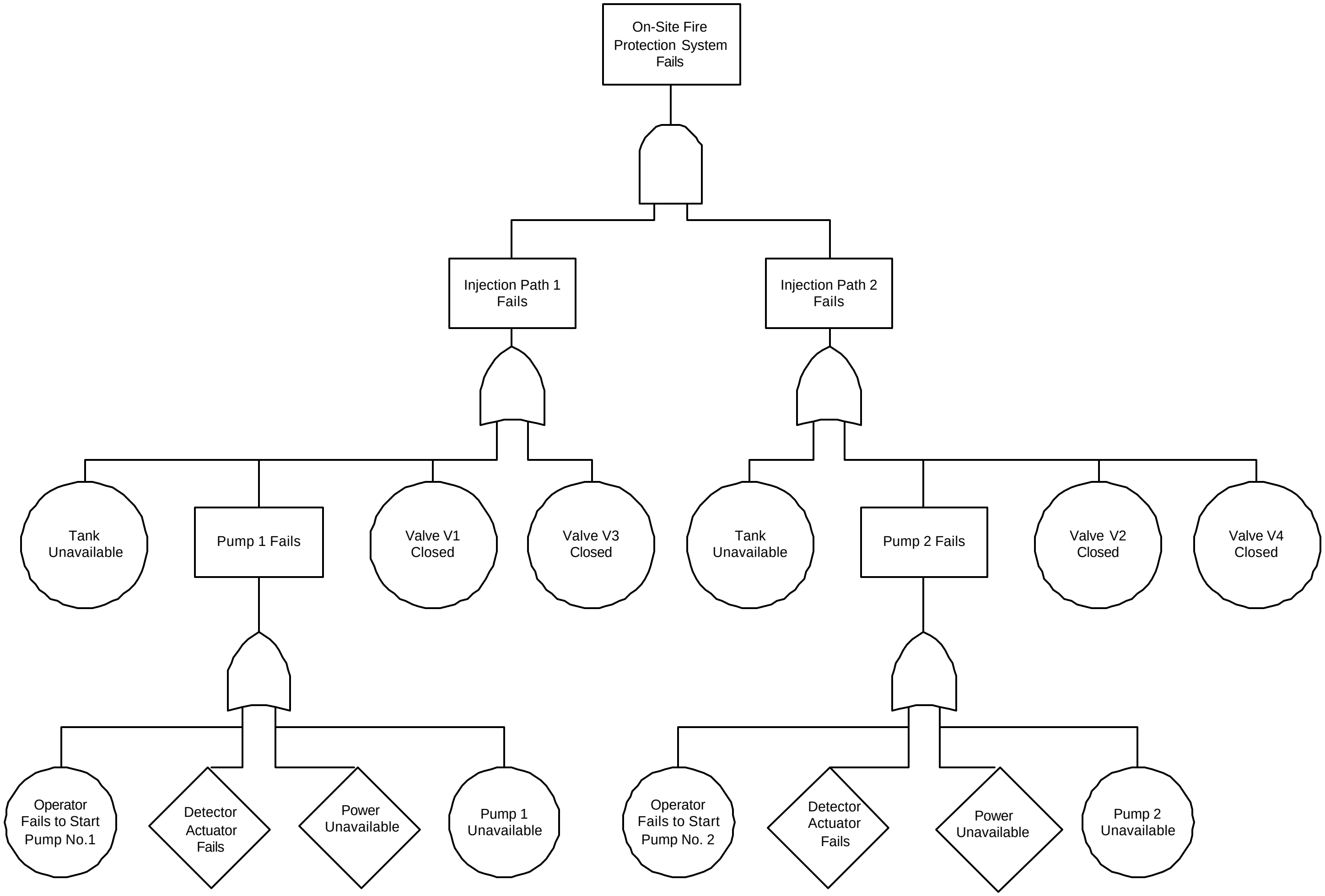
⇒ In this case, the pivotal event selected is the operation of the on-site fire protection system.

⇒ The failure of the on-site automatic fire protection system will be modeled using a fault tree.

On-Site Fire Protection System



Fault Tree for Pivotal Point in Event Tree



Fault Tree Quantification

- The evaluation of a fault tree can be accomplished in two major steps: ***reduction*** **and** ***quantification***

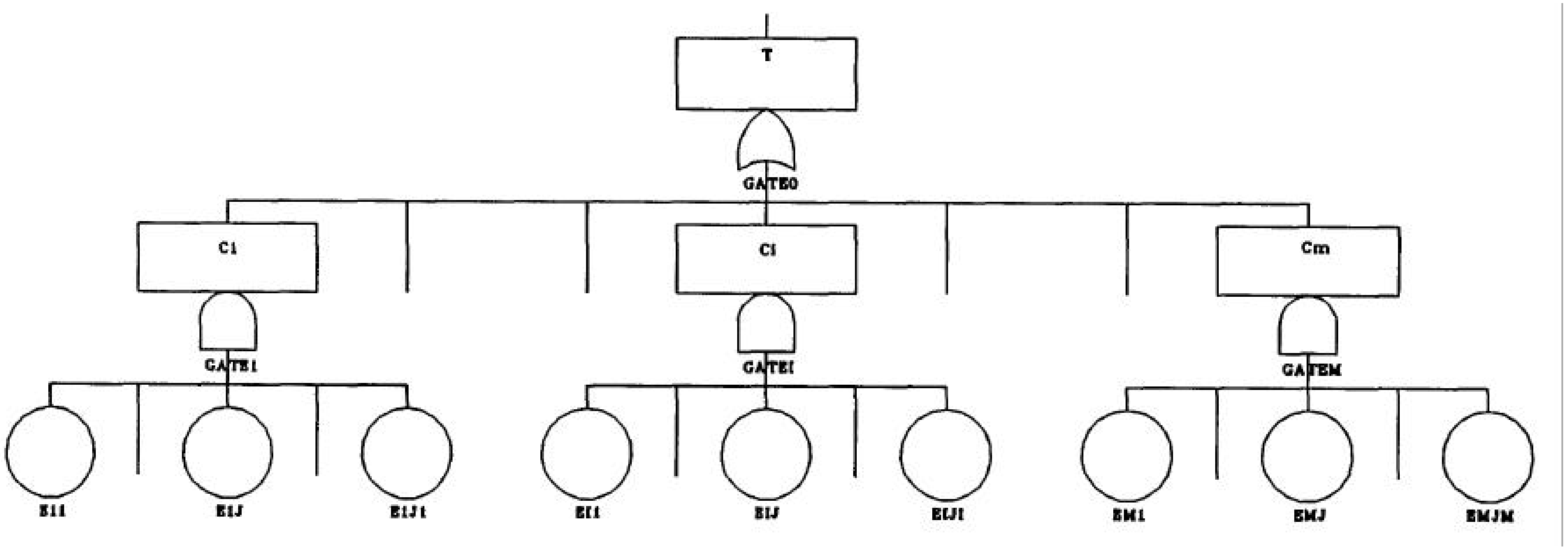
- **A set of primary events (failures) whose simultaneous occurrence guarantees the occurrence of the top event (failure) is called a** ***cut set***

- ***Minimal cut sets*** **are cut sets containing the minimum subset of primary elements whose simultaneous occurrence guarantees the occurrence of the top event**

- ***Boolean (or logic) reduction*** **of a fault tree has the objective of reducing the fault tree to an equivalent form which contains only minimal cut sets. This is accomplished by the application of the basic laws of Boolean algebra.**

- ***Quantification*** **of the fault tree is the evaluation of the probability of the top event in terms of the probabilities of the basic events using the reduced Boolean expression.**

Minimal Cut Set Representation of A Fault Tree



Minimal cut set 1 . . . Minimal cut set M

The simultaneous occurrence of all events in any minimal cut set guarantees the occurrence of the top event

Remaining PRA Steps (6,7,8)

For each initiating event, construct a risk scenario and an event tree; Then perform:

6. **Risk quantification for each pivotal event and each scenario and risk aggregation for all like end states.**

7. **Full uncertainty analysis and sensitivity analysis, as needed. Full uncertainty analysis requires propagation if all probability distributions through the PRA model using methods like the Monte Carlo method.**

8. **Risk importance ranking for risk reduction (as needed). Importance ranking of risk is performed to determine where risk reduction measures produce the largest risk reduction effect.**

Other Specialized Tasks in PRA

⇒ **Common-cause failure (CCF) or dependent failure analysis:**

Models of dependency among systems and components leading to failure probability that is higher than if systems and components are considered to be independent

⇒ **Human reliability analysis (HRA)**

Models accounting for human error prior to an accident, initiating an accident, or following an accident; Also, models accounting for human recovery actions

⇒ **External events analysis**

e.g., MMOD impact, lightning impact, etc.

PRA Computer Software

- **US Government sponsored software**
  - **SAPHIRE** - developed by INEEL under NRC sponsorship
  - **QRAS** - NASA sponsored software under development
- **Proprietary software -** Well-known packages:
  - **RISK SPECTRUM** - RELCON, Sweden
  - **NUPRA** - SCIENTECH, Inc., USA
  - **CAFTA/ETA** - SAIC, USA
  - **RISK MAN** - PLG, Inc., USA
  - **REVEAL** - SCIENTECH, Inc., USA